Possible Indicators of an Information Security Incident

- Sensitive, confidential, or mission-critical information is missing from your work area.
- File drawers or cabinets are open that should be closed.
- Confidential or sensitive documents have been moved or appear to have been used without the proper authorization.
- Software manuals are missing or moved.
- Your screen looks as if it is “melting,” mysterious shapes appear on your screen or in a document, or your document is converted to a template, etc.
- Your machine slows down suddenly and inexplicably.
- If your system displays the date and time you last logged onto the system and this date and time does not match the date and time you actually logged in.
- The system displays information indicating that there have been multiple invalid login attempts since your last valid login and you cannot account for them.
- Files and/or data have unexplainably been added, modified, or deleted.
- System audit reports, financial reports, or other reports in applications indicate suspicious or unauthorized activity.
- You come into the office, find your PC or terminal tuned on, and you are sure that you turned it off when you left the office.

What to Do When You Think an Incident Has Occurred

- Immediately report to the appropriate personnel any suspected information security incident.
- Confirm that an incident has indeed occurred or is likely to have occurred. For example, ask if the missing computer equipment, files, or documents were moved or borrowed; or confirm that your computer has a virus rather than a software or hardware error; etc.
- Be prepared to provide assistance if the incident requires an investigation.
- If the incident involves your computer (such as with a virus or intrusion), immediately stop using your computer and seek help from your technical support staff.
- Ensure that any reports required by your organization are completed and forwarded.
- **Complete GEN 1311 (CDSS INCIDENT REPORT)**

QUESTIONS?

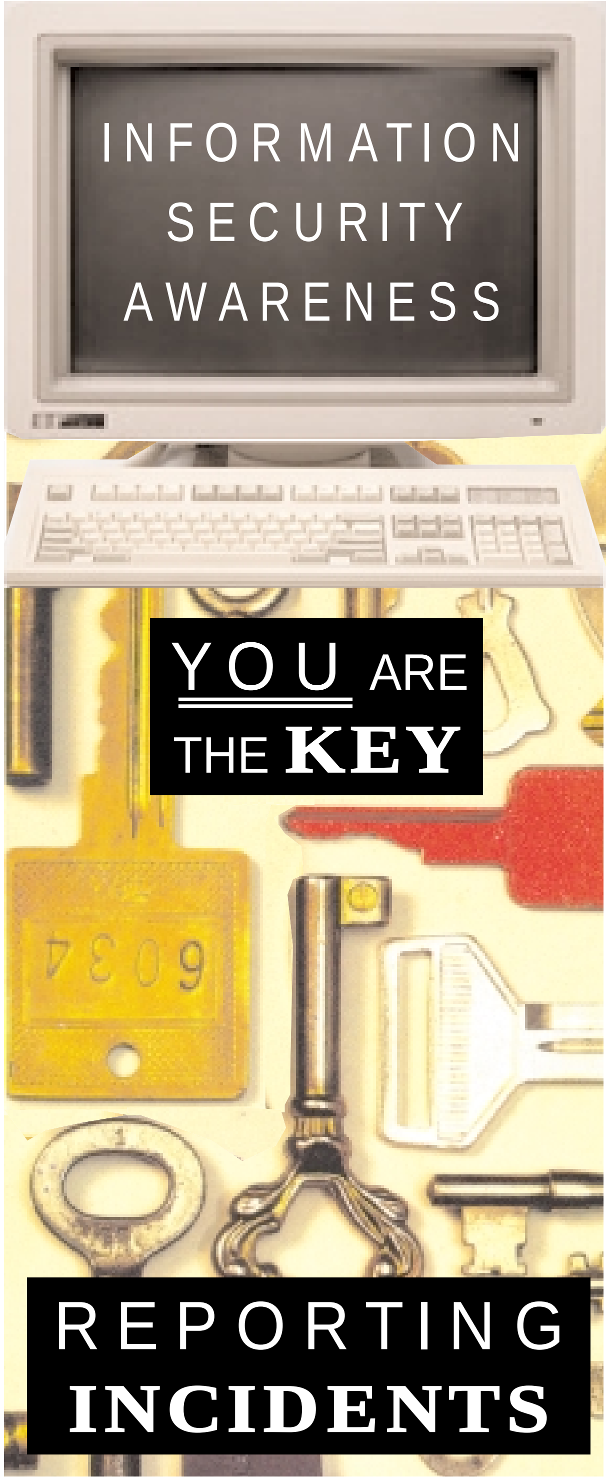
Call the Information Security and Management Systems Branch at (916) 657-3409

State of California
Gray Davis, Governor

Health and Human Services Agency
Grantland Johnson, Secretary

Department of Social Services
Rita Saenz, Director

PUB 312 (2/00)



INFORMATION SECURITY AWARENESS

YOU ARE THE KEY

REPORTING INCIDENTS

What is an Information Security Incident?

An information security incident is an event (intentional or unintentional) that causes the loss, damage to, destruction, or unauthorized disclosure of information assets.

Viruses

A virus is a software program that can damage data and/or inhibit the normal operation of a computer. It is not a distinct program and cannot run by itself. Examples of viruses include the Michelangelo series and the Microbes Virus.

Thefts of Information Assets

Thefts of information assets include thefts of anything used to process or store information (both electronic and hard copy) that occur at any location (work, while traveling, home, etc.).

Examples of information assets that should be reported when stolen include: confidential manuals or documents, personal computers, laptops, keyboards, software and software manuals, etc.

Misuse of Information Assets

The misuse of information assets is any unauthorized use or disclosure of any information asset. This can include intentional or unintentional acts. Examples of misuse can include tampering; use of information for purposes which violates any State or federal law, rule, regulation or policy; inappropriate use of the internet; sending e-mail chain letters; etc.

Destruction of Information Assets

Destruction of information assets includes an intentional or unintentional act that results in the loss of information assets (as a result of the incident the information is either temporarily or permanently unavailable and/or unrecoverable).

Examples of the destruction of information assets include a flood or fire that results in the destruction of computers and confidential manuals, a hard-drive crash, a confidential file that is left behind while traveling, a theft of a laptop containing confidential or sensitive data, etc.

Intrusions

Intrusions are intentional or unintentional acts that result in tampering, damage or unauthorized access to information assets. Intrusions can be “physical” or “electronic.” Intrusions can result in unauthorized access to paper documents as well as electronic information.

Examples of intrusions include breaking into the building, unauthorized access to paper documents, or accessing an automated system without authorization.